REMARKS

Claims 1-12 were presented for examination. In the Office Action (final) of March 27, 2006, claims 1-12 of the patent application were rejected. The rejections were upheld by the Board of Patent Appeals and Interferences in a decision of February 13, 2008. The claims, as amended, are listed above. No new matter has been added. Accordingly, claims 1-2, 6-12 and 15-17 are now pending for examination.

Applicant requests entry of the above amendments and reconsideration of allowance of the claims. Applicant responds to the rejections as follows:

§ 102 / § 103 Rejections

Claims 1-14 are rejected under 35 USC 103(a) as being unpatentable over Grawrock (US Patent No. 6,678,833) in view of Anderson (US Patent No. 6,161,177) (OA 3/27/08, para. 5).

Applicant respectfully traverses the rejections. In summary, while the claims compares a trusted BIOS source against an actual BIOS source used during boot up, Grawrock merely discloses calculating a boot block identifier, and Anderson checks for BIOS compatibility, but neither verifies against a trusted BIOS source.

Present Invention

Independent claim 1 includes limitations representative of independent claim 6. The present invention as recited in claim 1 includes a method for verifying a boot source in a computer system having a processor. The method includes storing a trusted boot source in a first register (i.e., a write-once register). The method also includes determining an actual boot source used by the processor each time the computer system boots. To do so, a location of a predetermined number of instructions used initially executed during boot up is examined. The method further includes storing an identity of the actual boot source in a second register. The method additionally includes comparing the actual boot source against the trusted boot source.

Prior Art

Grawrock generally discloses an integrated circuit devices with a trusted platform module and a blot block memory unit (Abstract). More particularly, Grawrock discloses that a boot block identifier is calculated for each start-up of the platform from boot information (3:62-63). Boot services can include a root of trust such as a boot block code executed at the start of the initialization process of the platform to locate, load and pass control of the BIOS (3:41-44). Thus, Grawrock discloses calculating boot block information.

Anderson generally discloses a motherboard adapted to receive a daughterboard containing a CPU coupled to a PCI bus (Abstract). Anderson discloses that the motherboard includes a BIOS that is compared against the daughterboard CPU (see 3:1-25). In the event that the data does not match, a floppy disc can be used to load the correct BIOS (see 3:1-25). Thus, Anderson discloses BIOS management.

Arguments

However, Grawrock fails to teach or suggest the invention as recited in claim 1. For example, in the method of verifying a boot source, claim 1 requires "comparing the trusted boot source against the trusted boot source." Advantageously, the computer system can confirm that the BIOS instructions used at boot up are obtained from a trusted boot source. On the other hand, Grawrock merely discloses calculating and storing a boot block identifier 330 within the TPM 230. The boot block identifier 330 is calculated just from a hash of boot information. Examiner asserts that Grawrock teaches writing the identity of the boot source in a register each time the computer system boots (OA 3/27/08, para. 5). However, the fact that Grawrock stores boot block identifier 330 in a register or even a non-volatile memory is of no consequence. The boot information of Grawrock is silent on a trusted boot source for use as a reference for comparison. Problematically, the boot block identifier of Grawrock does not allow the TPM to confirm that the actual boot source matches the trusted boot source, so the boot block identifier is untrusted, and worse, can be unscrupulous. Thus, the boot block identifier 330 of Grawrock fails to disclose the trusted boot source of claim 1.

Anderson fails to cure the deficiencies of Grawrock. Examiner asserts that Anderson teaches checking the boot source determined to ensure that the boot source is a known boot

source (OA 3/27/08, para. 5). Applicant respectfully disagrees. To the contrary, Anderson is directed towards managing multiple BIOS programs with respect to compatibility rather than verifying a BIOS with respect to security. To this end, although hardware data is compared to the BIOS identifying data, Anderson fails to contemplate requiring the BIOS identifying data to be trusted from a security point of view. In other words, a BIOS source that is compatible with the hardware data, but untrusted, can be used to compromise the computer system. Thus, the BIOS identifying data fails to disclose the trusted boot source of claim 1.

In fact, Anderson teaches away from claim 1. According to Anderson, in the case that the BIOS identifying data does not match the hardware data, Anderson teaches that a floppy disk can be used to reprogram the BIOS. There is no verification as to whether the substituted BIOS is trusted. Thus, Anderson cannot prevent untrusted BIOS from being used to boot up the computer system as provided by claim 1.

Neither Grawrock nor Anderson compare the actual boot source against the trusted boot source as in claim 1. Therefore, Applicant submits that independent claim 1, and all related dependent claims, are patentable over Grawrock and Anderson, either alone or in combination. Likewise, independent claim 6, and all related dependent claims, are patentable for at least the same reasons.

CONCLUSION

On the basis of the above remarks, reconsideration and allowance of the claims is believed to be warranted and such action is respectfully requested. If Examiner has any questions or comments, Examiner is respectfully requested to contact the undersigned at the number listed below.

Respectfully submitted,
SAWYER LAW GROUP LLP

Dated: March 27, 2008

/Joseph A. Sawyer, Jr./
Joseph A. Sawyer, Jr.
Attorney for Applicant
Reg. No. 30,801
(650) 475-1435